Technical Report **1755**
September 1997

RMON-2 Implementation and Results for the Automated Digital Networking System During JWID 97

E. W. Jacobs
M. E. Stell
L. M. Gutman

Naval Command, Control and Ocean Surveillance Center
RDT&E Division, San Diego, CA 92152–5001

Technical Report **1755**
September 1997

RMON-2 Implementation and Results for the Automated Digital Networking System During JWID 97

E. W. Jacobs
M. E. Stell
L. M. Gutman

Approved for public release; distribution is unlimited.

Naval Command, Control and Ocean Surveillance Center
RDT&E Division, San Diego, CA 92152–5001

NAVAL COMMAND, CONTROL AND OCEAN SURVEILLANCE CENTER
RDT&E DIVISION
San Diego, California 92152–5001

H. A. WILLIAMS, CAPT, USN
Commanding Officer

R. C. KOLB
Executive Director

ADMINISTRATIVE INFORMATION

The work detailed in this report was performed for the Networks Technology Branch (Code D827) of the Information Systems & Network Technology Division (Code D82) of the Communications Department (Code D80) of the Naval Command, Control and Ocean Surveillance Center RDT&E Division. Funding was provided by Space and Naval Warfare Systems Command (SPAWAR PD 13, LCDR Glen Darling) under program element 0603794N. This report covers work performed mainly during Summer 1997.

Released by
R. L. Merk, Head
Networks Technology
Branch

Under authority of
R. J. Kochanski, Head
Information Systems
& Network
Technology Division

SB

EXECUTIVE SUMMARY

This report documents the results obtained from implementation of Remote Monitoring (RMON) technology in the Automated Digital Networking System (ADNS) lab during the 1997 Joint Warrior Interoperability Demonstration (JWID 97). The report reviews the essentials of RMON and RMON-2 technology and describes the ADNS lab participation in JWID 97. The report then discusses the results of the RMON-2 historical data collection.

The utilization of RMON-2 in the ADNS lab for collection of historical network statistics was successful. The data collection over the demonstration period documented the amount of traffic (octets and packets), the type of traffic (link layer through application layer protocols), and the source and destination of traffic (link and network layer addresses). In particular, the data indicated the amount of routing protocol traffic used during periods of the test where the low-bandwidth RF links were primary utilized for multicast IP applications.

It is anticipated that the successful implementation of RMON-2 in this demonstration will provide a stepping stone towards the utilization of this technology for ADNS in the operational environment.

CONTENTS

Figures

Tables

1. INTRODUCTION

The Automated Integrated Communications System (AICS) is an advanced engineering program chartered to investigate the best ways of deploying commercial network management technologies in the Navy afloat networking environment and to determine the requirements and practices for adopting commercial network management to the Navy arena.

Briefly, network management is the monitoring and control of individual network resources (such as routers and links) and networks taken as a whole. Typical network management operations in the field are retrieving status and statistics, configuring network devices, and processing unsolicited messages by devices (e.g., alarms). The Remote Monitoring (RMON) standard provides an interface by which a network management application using the Simple Network Management Protocol (SNMP) directs the operation of stand-alone probes used to collect, collate, and report statistics on the packets traversing an attached network. The RMON standard, by in large, is concerned with the link-layer, e.g., Ethernet statistics. A recent extension, RMON-2, collects and collates statistics on protocols all the way up to the application layer. Thus, among the various kinds of network management functionality, RMON is concerned with the collection of network statistics.

AICS investigated RMON for the last 18 months with a view towards evaluating its effectiveness in an operational Navy afloat network. The effectiveness measures include: ease of use in an operational environment; the reliability of the data and implementations; and the timeliness and applicability of the statistical results to network performance management issues in an operational environment.

For the 1997 Joint Warrior Interoperability Demonstration (JWID 97), an RMON-2 probe was installed and utilized in the Automated Digital Networking System (ADNS) lab. Besides providing data points for the measures of effectiveness listed above, this experiment exposed engineers and managers of networking programs to the technology and gave them an opportunity to judge how well it might fit their systems. This paper reviews the operations and outcomes of that experiment.

The following section reviews RMON and RMON-2 technology. Section 3 gives an overview JWID 97 and ADNS, and how RMON-2 was implemented in the ADNS lab. Section 4 describes the results obtained using RMON-2 in the ADNS lab during JWID 97, and section 5 provides a summary and conclusion.

2. RMON and RMON-2 TECHNOLOGY

Remote network monitoring devices, often called monitors or probes, are instruments that aid in network management. A RMON probe consists of a) an interface that listens to a local area network (LAN) in a promiscuous mode and, b) an implementation of an SNMP agent supporting the the RMON management information base (MIB) or the RMON-2 MIB. Currently, RMON probes with Ethernet, token-ring, and Fiber Distributed Data Interface (FDDI) interfaces are available, although this document only discusses Ethernet RMON probes.

There are two RMON standards: RMON (reference 1) and an extension to RMON called RMON-2 (reference 2). These standards extend the information contained in the MIB-II standard (reference 3) and provide a far more detailed description of the traffic traveling on a LAN. RMON includes the capability to quickly access link layer (i.e., Ethernet layer) statistics. It also includes the capability to filter and selectively capture packets, thereby enabling analysis of higher network layers in a less convenient and less practical manner. The RMON-2 standard incorporates quick access to statistics all the way up to the application layer. Within the last 6 months COTS probes that conform to most of the RMON-2 standard have become available (reference 4). The RMON and RMON-2 MIBs describe the information that the probes maintain and make available to network management programs that issue appropriate SNMP requests. A RMON probe monitors only the LAN to which it is attached. It is called a *remote* network monitoring device because the information the probe collects can be retrieved remotely by management applications via SNMP requests. For general information on the SNMP manager/agent paradigm, see, for instance, reference 8.

To provide a better description of the type of information that can be obtained from a RMON probe, some of the groups in the RMON and RMON-2 MIBs are briefly described in the following paragraphs.

As described below, groups contained in the RMON MIB include the Ethernet statistics, history, host, hostTopN, matrix, filter, capture, alarm, and event groups.

Ethernet Statistic Group. This group contains statistics describing the Ethernet packets detected on the monitored LAN. These statistics include the number of Ethernet packets, octets, broadcast packets, multicast packets, cyclic redundancy code errors, fragments, jabbers, collisions, oversized packets, undersized packets, and packets of various sizes.

Ethernet History Group. The Ethernet history group records periodic statistical samples from an Ethernet LAN and stores them for later retrieval. This is useful in reducing the SNMP traffic between the SNMP management application and the probe in cases where they are separated by a busy or low-bandwidth link. A manager can use the history control group to configure the statistics collected in this group.

Host Group. The host group contains statistics associated with each Ethernet host discovered on the network. Contained in this group is a list of source and destination media access control (MAC) addresses seen in good packets promiscuously received from the LAN. Statistics included in this group include packets and octets sent and received by a given MAC address, and errors, broadcast packets, and multicast packets sent by a given MAC address.

HostTopN Group. The hostTopN group is used to prepare reports that describe the Ethernet hosts that top a list ordered by one of their statistics included in the host group over a specified time interval.

Matrix Group. The matrix group stores statistics for conversations between sets of two addresses. The statistics include a count of packets, octets, and errors. To facilitate easy retrieval of data by an SNMP management application, the group contains tables indexed by source/destination and by destination/source addresses.

Filter and Packet Capture Groups. The filter and packet capture groups work in conjunction to allow a method for easily and flexibly capturing a desired subset of the packets on the monitored LAN.

Alarm and Event Groups. The alarm group monitors variables in the probe and compares them to configured thresholds. If the monitored variable crosses a threshold, an event is generated. A hysteresis mechanism is implemented to limit the generation of alarms. Once again, this group is useful in reducing the SNMP traffic between the SNMP management application. The alarm group works in conjunction with the the event group that controls the generation and notification of events from the probe.

As described below, groups contained in the RMON-2 MIB include the protocol directory, protocol distribution, network layer host, network layer matrix, application layer host, application layer matrix, and user history groups.

Protocol Directory Group. This group identifies the protocols that the probe can monitor.

Protocol Distribution Group. This group contains statistics describing the number of packets and octets of each protocol detected on the monitored LAN.

Network Layer Host Group. This group contains statistics describing the number of packets and octets to and from each network address identified in packets detected on the monitored LAN.

Network Layer Matrix Group. This group contains statistics describing the number of packets and octets sent between pairs of network addresses

identified in packets detected on the monitored LAN. As with the Ethernet layer matrix group, to facilitate simple retrieval of data by an SNMP management application, the group contains tables indexed by source/destination and by destination/source addresses. In addition to the nlMatrixTable, the network layer matrix group also contains the nlMatrixTopNTable, which allows easy documentation of the network layer conversations generating the most traffic.

Application Layer Host Group. This group contains statistics describing the number of packets and octets of each protocol sent to and from each network address identified in packets detected on the monitored LAN. The application layer host group is not limited to protocols identified with layer 7 of the OSI network model (reference 5), but, in general, contains statistics for protocols from layers three through seven.

Application Layer Matrix Group. This group contains statistics describing the number of packets and octets of each protocol sent between pairs of network addresses identified in packets detected on the monitored LAN.

User History Group. The user history group provides a more general means than the Ethernet history group, of storing historical statistics on the probe. This group allows for identification of the time interval, the total length of time, and the variable to store. As with the Ethernet history group, the user history group reduces the required number of communications between an SNMP management application and the probe.

Through the design of the RMON and RMON-2 MIBs as described above, an RMON probe can provide a network manager with both real-time information, and with information gathered over prolonged collection periods. Real-time information is typically used by network managers for pro-active and fault management, while the information gathered over prolonged periods is typically used for performance management. To effectively utilize the real-time information made available by the probe, an RMON/RMON-2 SNMP management application with a graphical user interface is desired. For collection and presentation of historical data, the only requirements are a general-purpose SNMP utilities package and a general-purpose plotting package in combination with some simple scripts to sort out the data. As will be detailed in section 4, in the ADNS lab during JWID 97, RMON-2 was utilized only for the collection of historical data. For a summary of an implementation where information provided by an RMON-2 probe was utilized for real-time network management functions, see reference 6.

3. JWID 97 and ADNS

The first part of this section provides general background on JWID 97 and ADNS, and the role ADNS played in the demonstration. The end of this section summarized the RMON-2 setup in the ADNS lab.

JWID 97 was a United States and Allied Coalition operation led by the Commander, Carrier Group Six who acted as the Commander, Coalition Task Force (CCTF) conducting Combined Operations at the Joint Component Commander Level. There were many purposes for JWID 97, but most relevant to this report was that of demonstrating the ability of commercial off-the-shelf/government off-the-shelf (COTS/GOTS) technology to provide constant data exchange with deployed elements at sea, and demonstrating innovative information management technology that enhances data delivery to and from Joint Warriors. Commander-in-Chief United States Atlantic Command (CINCUSACOM) was the host CINC operating from the Joint Battle Center (JBC) at the Joint Training Analysis and Simulation Center (JTASC) in Suffolk Virginia. The CCTF and his staff operated from USS *John C. Stennis* (CVN 74). JWID 97 took place from 7 July to 31 July 1997.

The purpose of ADNS is to provide Navy afloat platforms with IP services by means of a system based on the incorporation of COTS and GOTS hardware and software with currently installed RF transmission resources. COTS IP routers using the Open Shortest Path First/Multicast Open Shortest Path First (OSPF/MOSPF) routing protocols are used to minimize the distribution of routing information. As figure 1 shows, between the IP router and RF radios reside Channel Access Protocol (CAP) devices and the CAP Router Interface Unit (CRIU). (Note: Not all the devices which make up the ADNS architecture are shown in figure 1. For a more complete description of the ADNS architecture, see reference 7.) The CRIU provides the physical interface between the IP router and the CAP for each media and performs data buffering and framing as required to ensure efficient data flow across the RF links. The ADNS system can support multiple RF resources. This is indicated in figure 1 where three different RF radios are shown, in particular, 16-kHz bandwidth ultra high frequency demand-assigned multiple access satellite communications (16-kHz UHF DAMA SATCOM), a resource supported by virtually all U.S. Navy ships.

For JWID 97, six ADNS sites with assets similar to that shown in figure 1 were configured to communicate over 16-kHz UHF DAMA SATCOM. The six ADNS sites included five simulated "ships" and one actual ship at sea. The five simulated ships were the HMAS *Perth* (Australia), HMCS *Vancouver* (Canada), HMS *Grenville* (United Kingdom), USS *Nassau* (NRaD), and USS *Doyle* (Charleston, SC). The one actual ship at sea, HMNZS *Canterbury* (New Zealand), communicated directly over a separate channel with NRaD, where its traffic was then routed to 16-kHz UHF DAMA SATCOM. The sites could also communicate with shore sites worldwide through NRaD's

connection to the Coalition Wide Area Network (CWAN). Routing was configured so as to direct traffic from the interior LANs to the correct remote destination, whether it was another "ship" or another part of the world. Ship-to-ship traffic went directly over the RF media. Traffic destined for a shore-based site was sent from one of the "ships" over the RF media to NRaD where the traffic was forwarded to its ultimate destination over the CWAN.

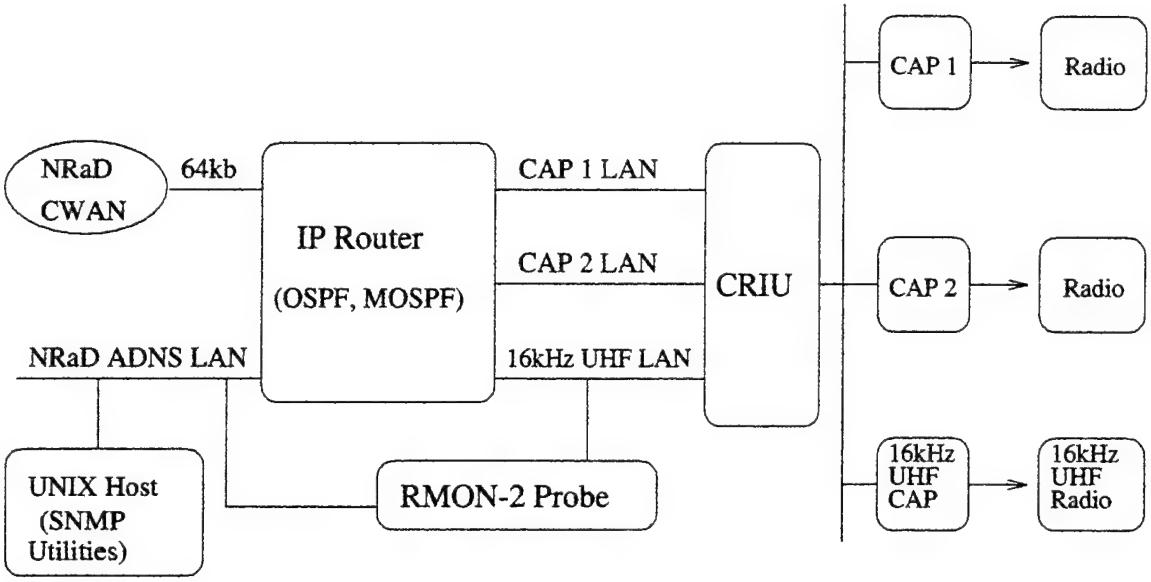

Figure 1. ADNS setup.

A goal of this effort was to demonstrate that standard IP-capable applications (in particular, several multicast applications, X-400, Joint Maritime Command Information System (JMCIS) Packet Assembler/Disassembler (PAD), FTP, and Chat) can communicate over low-bandwidth RF media and on to the CWAN. A prerequisite for this communication is that the IP routers successfully exchange (over the RF media) the required routing information. As the number of routers (i.e., sites) increases, the amount of required routing information also increases, therefore a significant fraction of the available bandwidth can be taken up for the exchange of routing information. Therefore, collecting statistics on routing protocol traffic during the demonstration was of primary interest.

In figure 1, note that between the IP router and CRIU, there exists a LAN that carries only packets routed over a specific RF resource. A RMON-2 probe with two Ethernet interfaces, one acting as a management interface, and the other as the monitoring interface (reference 4), was connected as shown in the figure 1. The monitoring interface was connected to the LAN carrying data routed over 16-kHz UHF DAMA SATCOM, while the management interface was connected to the LAN local to the NRaD ADNS lab. In this way, the probe was able to monitor all outgoing traffic routed by the IP router to 16-kHz UHF DAMA SATCOM, and all incoming data

passed by the 16-kHz UHF CAP from remote 16-kHz UHF DAMA SATCOM sites.

General SNMP utilities hosted on a UNIX workstation residing on the LAN local to the NRaD ADNS lab were used to configure and collect statistics from the RMON-2 probe via the probes management interface. The nlMatrixTopNTable was configured to record the top 50 network layer conversations in 30-minute intervals, and scripts using the general SNMP utilities were scheduled to periodically collect this information. Because the multicast applications communicating between the NRaD ADNS lab and the other JWID 97 TGAN sites were a primary focus of the ADNS effort, scripts were scheduled to periodically collect information from the nlMatrixDSTable relevant to the network layer traffic sent to the multicast addresses of interest. The amount of traffic of each protocol, particularly routing protocol traffic, was also a primary interest, therefore information was periodically collect from the protocolDistStatsTable. Finally, to provide link layer traffic information, data were also collected from the etherStatsTable.

4. RESULTS

At the conclusion of the JWID 97 demonstration, scripts were written to sort and manipulate the data collected from the nlMatrixTopNTable, nlMatrixDSTable, and protocolDistStatsTable. There were three areas in particular where the collected data yielded useful information. These three areas were: distribution of traffic by protocol (in particular, OSPF traffic); characterization of multicast application traffic; and the source of both unicast and multicast traffic.

Figures 2 through 9 show data collected from the protocolDistStatsTable summarizing the distribution of traffic by protocol. The data were collected from 29 July 0000 GMT to 31 July 1500 GMT using 3-hour bins up to 29 July 1800 GMT, and 1-hour bins, thereafter. The octet rates indicated in the figures represent the average octet rate over the time period of each bin. The testing periods (i.e., the time intervals when some or all of the sites were communicating over the RF links) began at approximately 1200 GMT and lasted approximately 12 hours on 29 and 30 July, and 3 hours on 31 July. The increase in traffic during these testing periods is clearly evident in figures 2 through 9.

Layer 2 Ethernet traffic, essentially all the traffic transmitted on the LAN, is shown in figure 2. Layer 3 IP traffic shown in figure 3 indicates that approximately 80% of the Ethernet octets were encapsulated in IP packets. Layer 4 TCP, UDP, OSPF, IGMP, and ICMP traffic is shown in figures 4 through 8. During the testing period, more UDP traffic was transmitted than any other layer 4 protocol. This was because much of the traffic during the testing period was generated by IP multicast applications. Note that on 30 and 31 July, significant TCP traffic was also transmitted over specific time intervals.

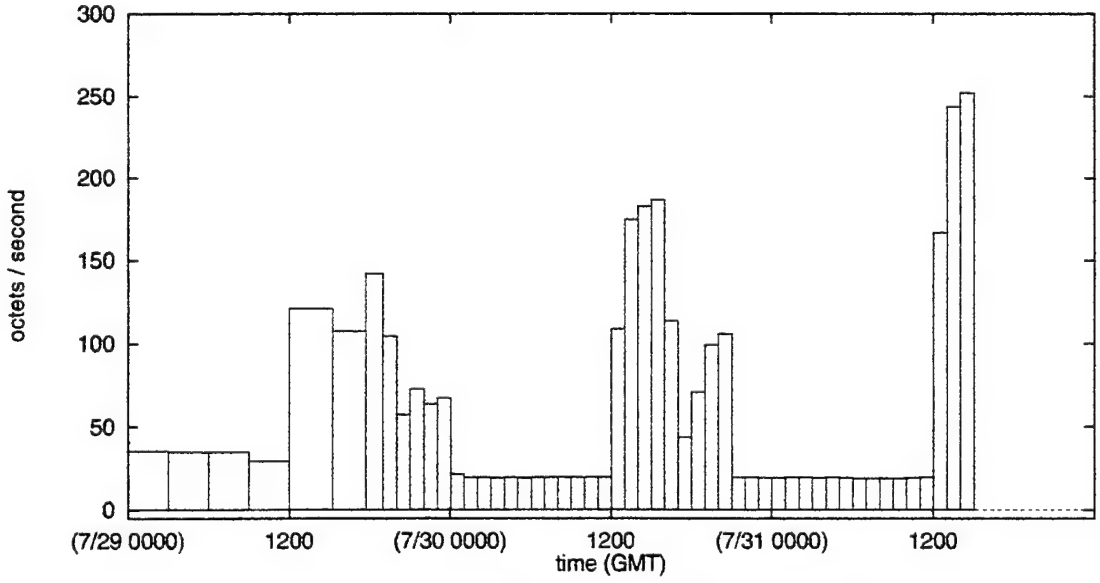

Figure 2. Ethernet traffic on 16-kHz UHF CAP LAN.

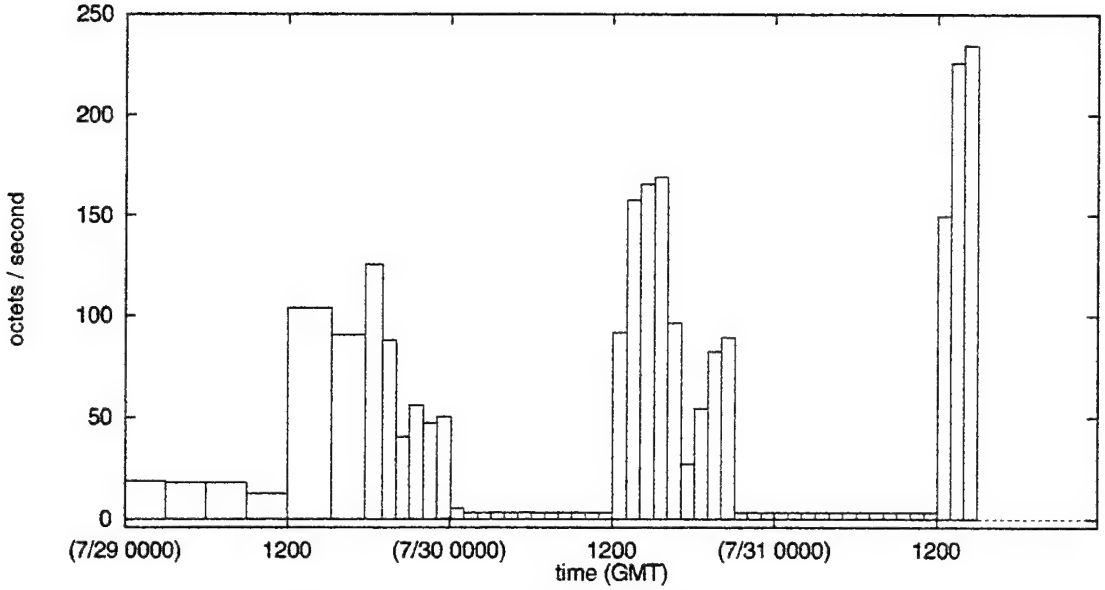

Figure 3. IP traffic on 16-kHz UHF CAP LAN.

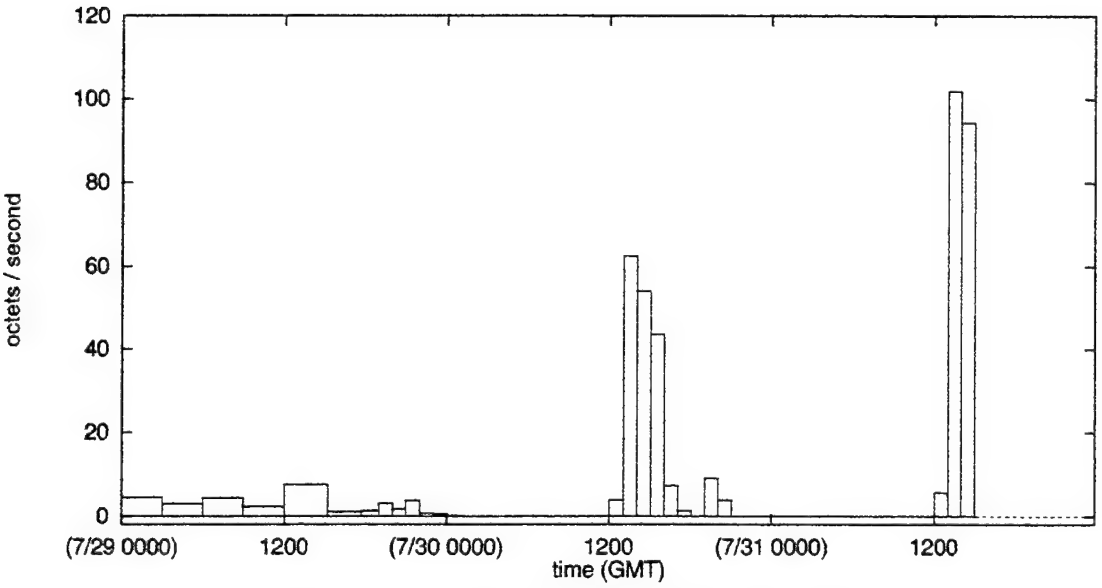

Figure 4. TCP traffic on 16-kHz UHF CAP LAN.

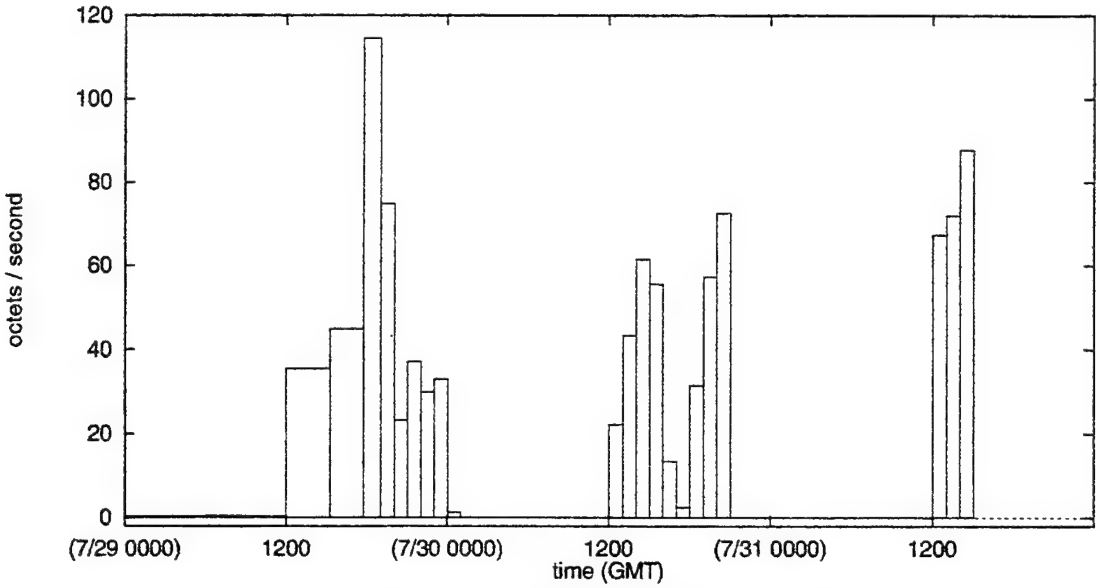

Figure 5. UDP traffic on 16-kHz UHF CAP LAN.

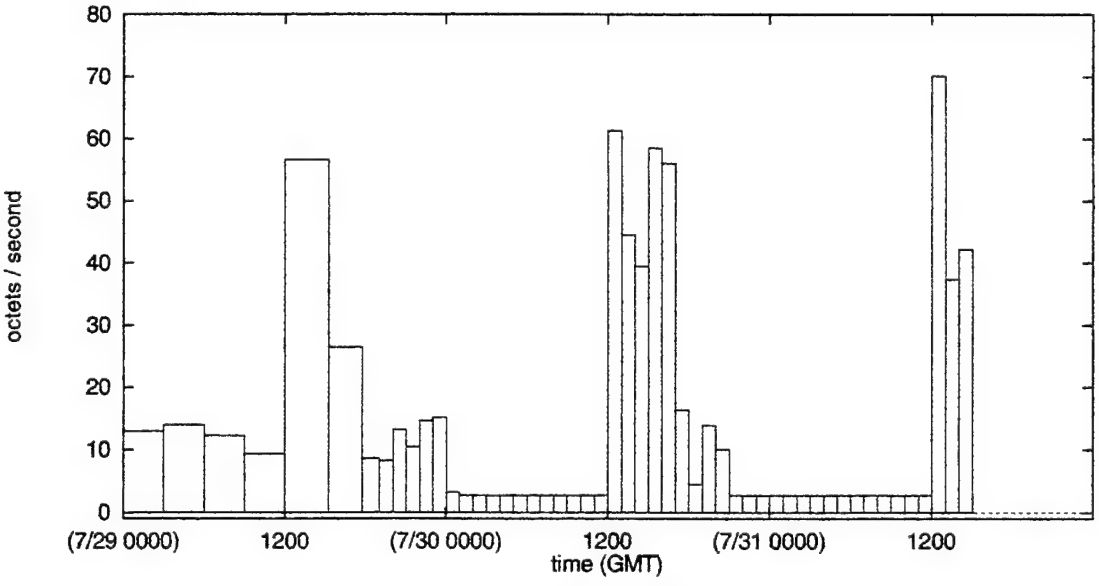

Figure 6. OSPF traffic on 16-kHz UHF CAP LAN.

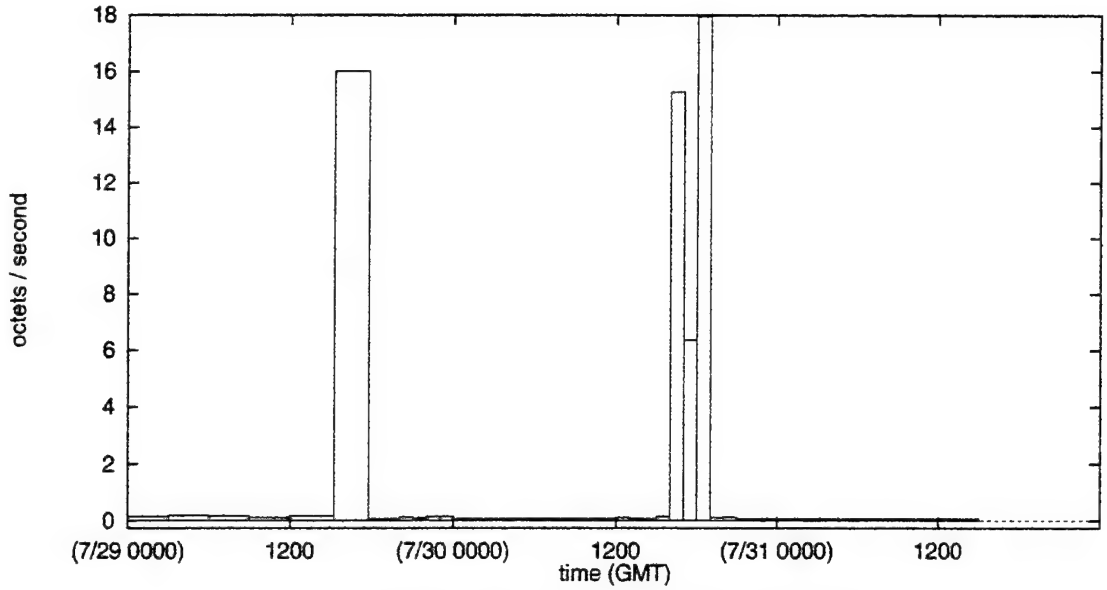

Figure 7. IGMP traffic on 16-kHz UHF CAP LAN.

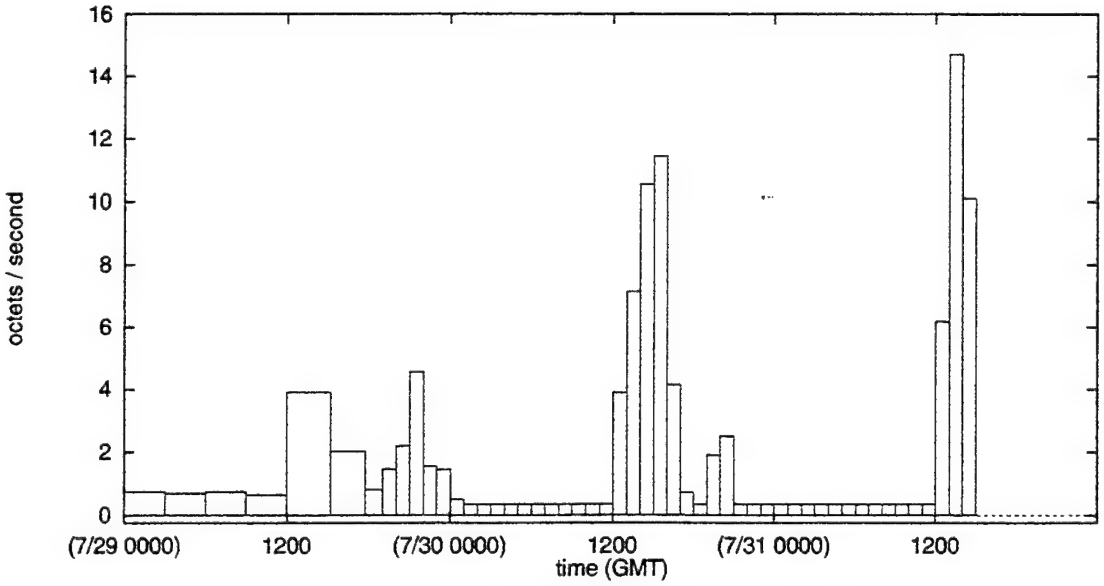

Figure 8. ICMP traffic on 16-kHz UHF CAP LAN.

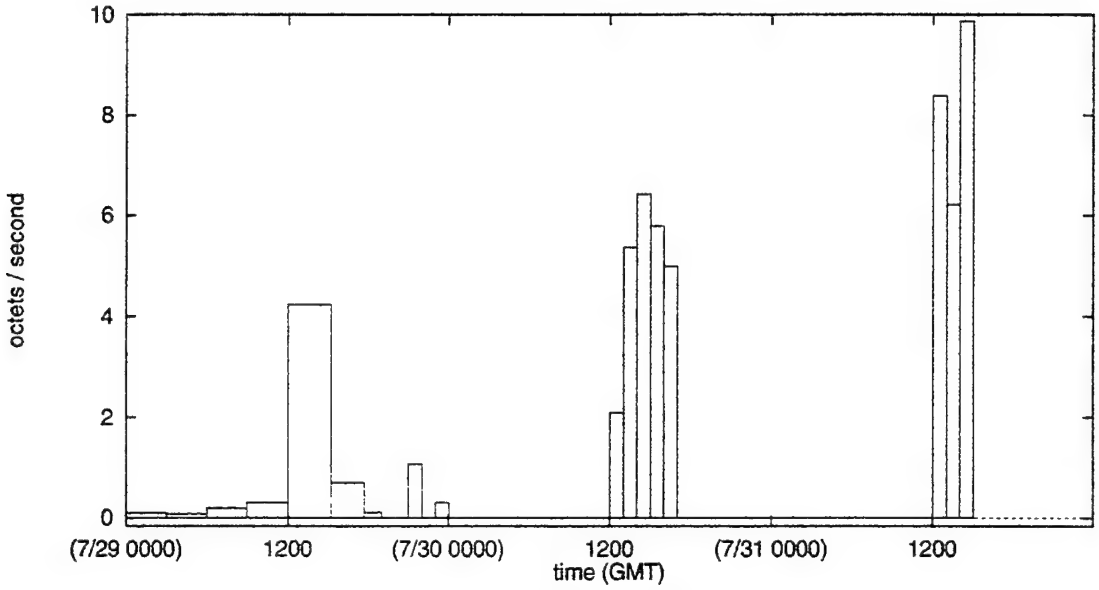

Figure 9. DNS traffic on 16-kHz UHF CAP LAN.

As stated previously, statistics on OSPF traffic were of particular interest. Comparison of figure 6 with figure 2 shows that a significant fraction of the total traffic on the LAN was OSPF traffic.

All six sites were actively participating on the 16-kHz UHF network during three test-period intervals, 29 and 30 July (1200 to 1700 GMT) and 31 July (1200 to 1500 GMT). Table 1 summarizes data from figures 2 and 6 for these periods.

Table 1. Summary of ratio of OSPF to total traffic during specific time intervals.

Time interval	Ethernet Octets	OSPF Octets	%OSPF
29 Jul 1200 - 1800 GMT	2463782	896822	36.4
30 Jul 1200 - 1700 GMT	2757243	934546	33.9
31 Jul 1200 - 1500 GMT	2383419	538330	22.6
Total	7604444	2369698	31.2

Approximately 30% of the total traffic flowing from the router to the CRIU and then to the 16-kHz UHF media was OSPF protocol traffic. This is, in part, due to the fact that total traffic during these time intervals was rather light, approximately 1200 bits per second.

The only other standard protocols using non-trivial fractions of the bandwidth were two layer 3 protocols, IGMP and ICMP, shown in figures 7 and 8, and the application layer protocol DNS shown in figure 9. Figure 9 shows the sum of DNS using both TCP and UDP transport encapsulation. The spikes in the IGMP traffic shown in

figure 7 are a result of Emission Control (EMCON) testing. During EMCON, ships can receive but not transmit data, a procedure which IP cannot normally preform. During EMCON, ships cannot transmit the required multicast group membership information. Therefore, the CRIU is programmed to send IGMP packets to the router indicating that it is a member of particular multicast groups so that the OSPF router will forward IP multicast packets. As a result, IGMP traffic appears during periods of EMCON testing.

In figures 10 through 13, data summarizing the amount of traffic sent to the multicast addresses associated with specific multicast applications are presented. Figures 10, 12, and 13 were compiled from data collected from the nlMatrixDSTable, while figure 11 was compiled from data collected from the nlMatrixTopNTable. Figures 10 and 11 show significant amounts of X400 and JMCIS-PAD multicast traffic, figure 12 shows far less multicast chat traffic, and figure 13 shows that a significant amount of multicast FTP traffic was present during only three 1-hour intervals. Comparison of these figures with figure 5 shows that the majority of the UDP traffic consisted of these multicast applications. In the paragraphs below, the source of this multicast traffic is discussed.

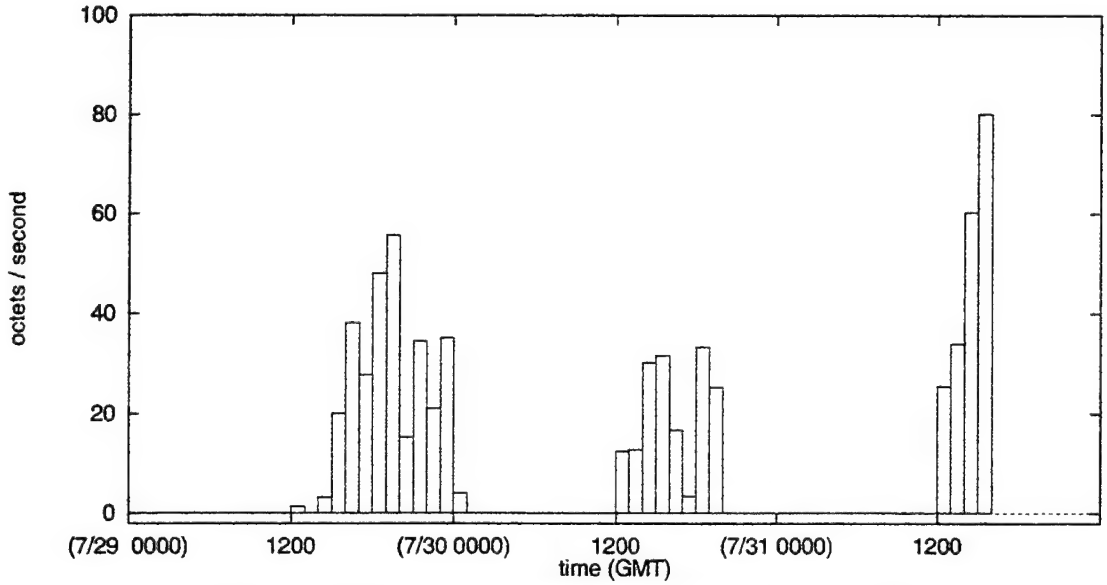

Figure 10. Multicast X400 traffic on 16-kHz UHF CAP LAN.

Tables 2 and 3 provide information on the source of traffic. Tables 2 and 3 were derived from data collected from etherStatsTable during the testing period as described above. From table 2, note that over twice as much traffic on the 16-kHz UHF LAN originated from the IP router than from the CRIU, indicating that the ADNS lab at NRaD sent out substantially more traffic than it received. The traffic sent out from the NRaD node included traffic from the ADNS local LAN, the New Zealand node, and the CWAN. A bit more can be learned from the destination MAC address data in table 3, where 28.8% of the traffic was unicast traffic destined for the IP router, 20.6%

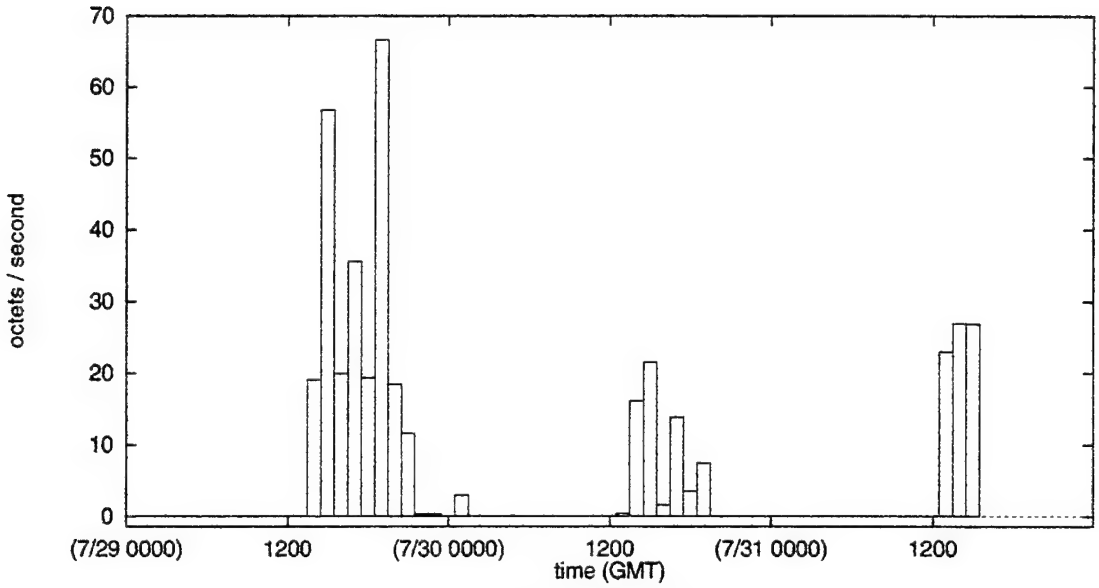

Figure 11. Multicast JMCIS-PAD traffic on 16-kHz UHF CAP LAN.

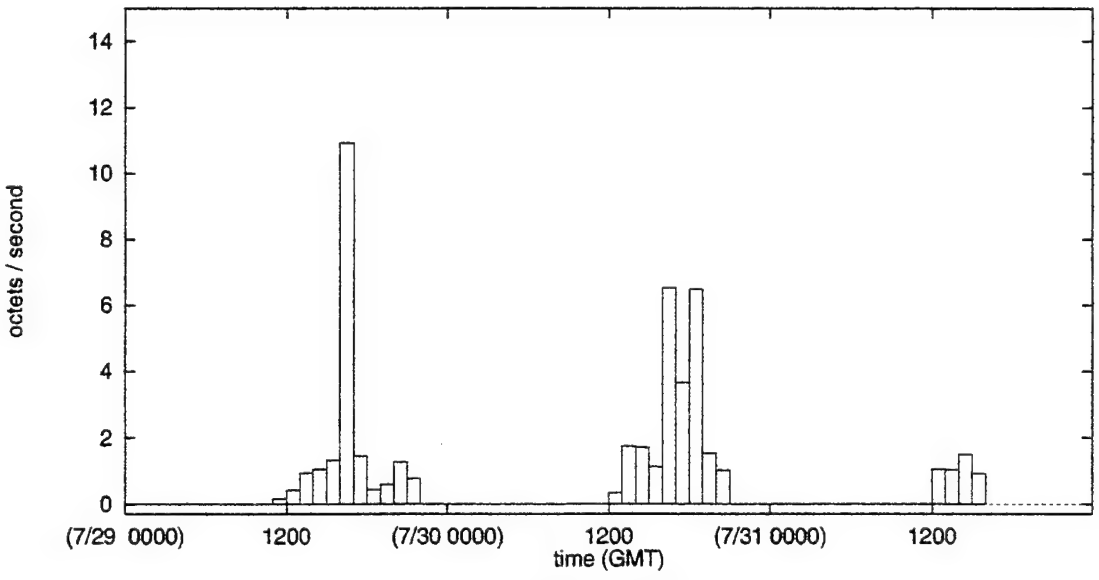

Figure 12. Multicast chat traffic on 16-kHz UHF CAP LAN.

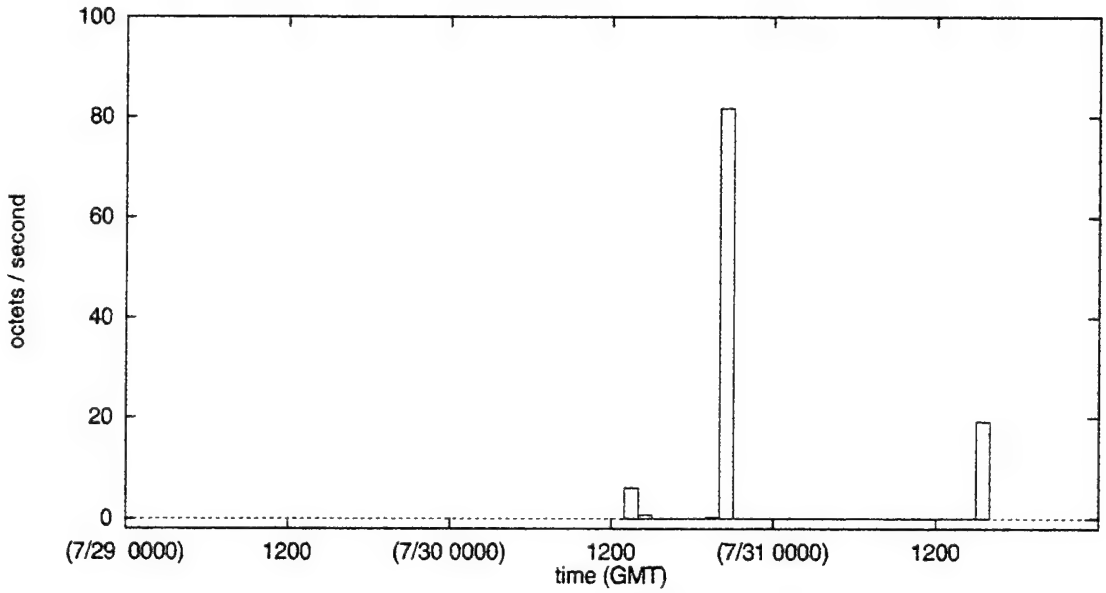

Figure 13. Multicast FTP traffic on 16-kHz UHF CAP LAN.

of the traffic was unicast traffic destined for remote sites, 37.1% of the traffic was X-400, FTP, Chat, and JMCIS-PAD multicast, and 12.5% of the traffic was multicast OSPF (MOSPF). It is important to mention that, as a means of checking its interface, the Proteon IP router sent a packet to itself every 4 seconds. As as result, more than half of the unicast traffic with the IP router as the destination MAC address also had the IP router as the source MAC address. Note that the traffic destined for remote sites is indentified by the MAC address of the remote site's CAP. This is a result of the ADNS implementation wherein, in responds to Address Resolution Protocol (ARP) requests from the local IP routers, the CRIU returns the remote CAP MAC address (for packets destine for the corresponding remote IP router). Also, note that the data of table 1 includes all OSPF traffic, whereas the data in table 3 is MOSPF traffic only.

Table 2. Fraction of octets in Ethernet packets with a given source MAC address.

Source MAC Address	% Traffic
IP Router	69.8
CRIU	30.2

By examining network layer statistics, insight into the source of the application multicast traffic can be gained. These statistics, compiled from the nlMatrixDSTable and the nlMatrixTopNTable, are shown in table 4. The New Zealand traffic was routed through NRaD, therefore it can be inferred from table 4 that 65.1% of the IP application multicast traffic was sent out from NRaD, while 28.9% of the IP application

Table 3. Fraction of octets in Ethernet packets with a given destination MAC address.

Destination MAC Address	% Traffic
IP Router	28.8
Canada CAP	10.7
Australia CAP	5.8
UK CAP	3.0
Charleston CAP	1.1
Total CAP	20.6
Application Multicast	37.1
OSPF Multicast	12.5
Total Multicast	49.6
Broadcast	1.0

multicast traffic was sent from remote sites to NRaD. In addition, table 4 indicates 6.1% of the IP application multicast traffic had the CRIU as its source IP address. This traffic is the IGMP traffic discussed above in reference to figure 7.

The data presented in this report, collected from various RMON and RMON-2 tables sampling both link and network layer statistics, are relatively self-consistant. Small inconsistancies in the data are expected because of slightly different collection intervals for the various tables. The self-consistancy between the various tables yields confidence that the probe was accurately collecting and tabulating (essentially) all the packets/octets on the LAN.

Table 4. Fraction of multicast IP octets with a given IP source address.

Source IP Address	% Traffic
NRaD	37.2
New Zealand	27.9
Australia	23.0
Canada	5.1
Charleston	0.6
UK	0.2
CRIU	6.1

5. SUMMARY AND CONCLUSION

This report documents the results obtained from an implementation of RMON-2 technology in the NRaD ADNS lab during JWID 97. The RMON-2 technology was utilized to collect historical data for review of network utilization during the demonstration.

The utilization of RMON-2 for collection of historical data was successful. Data collected over the demonstration period documented the amount of traffic (octets and packets), the type of traffic (link layer through application layer protocols), and the source and destination of traffic (link and network layer addresses). In particular, the data indicated that during periods of testing when the 16-kHz UHF links were utilized primarily for multicast IP applications, approximately 30% of the traffic was OSPF routing traffic. The OSPF traffic can be adjusted via a number of OSPF parameters. By adjusting these parameters to decrease the amount of OSPF traffic, the speed with which routers can form adjacencies with each other, and the speed at which routers detect and correct RF media failures is adversely effected. Therefore, determining the best set of OSPF parameters is an optimization problem. Studies of this optimization problem for specific RF media would be useful in obtaining the maximum time-averaged available bandwidth. Beyond illuminating OSPF traffic issues, another area where the collected data yielded particularly useful information was the amount and source of multicast application traffic.

Collection of these statistics will help explain the network requirements for ADNS in future scenarios, especially for cases where the relevant networks will operate in the operational environment over extended time periods. It is anticipated that the success of the implementation of RMON-2 in this demonstration will provide a stepping stone towards the utilization of this technology in the operational environment.

6. REFERENCES

1. S. Waldbusser. 1995. "Remote Network Monitoring Management Information Base," RFC1757.

2. S. Waldbusser. 1997. "Remote Network Monitoring Management Information Base Version 2 using SMIv2," RFC2021.

3. K. McCloghrie, M. Rose. 1991. "Management Information Base for for Network Management of TCP/IP-based Internets: MIB-II," RFC1213.

4. Technically Elite, Inc., San Jose, CA. http://www.tecelite.com/index.html

5. J. D. Day and H. Zimmerman. 1983. "OSI Reference Model," *Proceedings of the IEEE*, vol. 71, pp. 1334–1340.

6. E. W. Jacobs, L. M. Gutman, R. H. Cheng, and M.S. Lavelle. 1997. "RMON-2 Implementation and Results for COMPASS During JWID 97," NRaD TR1753. Naval Command, Control and Ocean Surveillance Center RDT&E Division, San Diego, CA.

7. R. Casey. 1997. "ADNS Implementation Working Paper," ADNS/WBS 1/WP/006 Rev1. (Available from authors upon request).

8. M. T. Rose. 1994. *The Simple Book, An Introduction to Internet Management*, P T R Prentice Hall, Englewood Cliffs, NJ.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1997	Final: August 1997

4. TITLE AND SUBTITLE
RMON-2 IMPLEMENTATION AND RESULTS FOR THE AUTOMATED DIGITAL NETWORKING SYSTEM DURING JWID 97

5. FUNDING NUMBERS
PE: 0603794N
AN: DN306547
WU: X2091

6. AUTHOR(S)
E. W. Jacobs, M. E. Stell, L. M. Gutman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Command, Control and Ocean Surveillance Center (NCCOSC)
RDT&E Division (NRaD)
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER
TR 1755

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Space and Naval Warfare Systems Command
Washington, D. C. 20363–5100

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The Automated Integrated Communications System (AICS) is an advanced engineering program chartered to investigate the best ways of deploying commercial network management technologies in the Navy afloat networking environment and to determine the requirements and practices for adopting commercial network management to the Navy arena. For the 1997 Joint Warrior Interoperability Demonstration (JWID 97), a RMON-2 probe was installed and utilized in the ADNS lab. Besides providing data points for the measures of effectiveness, this experiment exposed engineers and managers of networking programs to the technology and gave them an opportunity to judge how well it might fit their systems. This paper reviews the operations and outcomes of that experiment.

14. SUBJECT TERMS
Mission Area: Command, Control, and Communications
operational network management
Automated Digital Networking System (ADNS)
Joint Warrior Interoperability Demonstration (JWID)

15. NUMBER OF PAGES
27

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS REPORT

21a. NAME OF RESPONSIBLE INDIVIDUAL	21b. TELEPHONE *(include Area Code)*	21c. OFFICE SYMBOL
E. W. Jacobs	(619) 553-1614 e–mail: jacobs@nosc.mil	Code D364

INITIAL DISTRIBUTION

Code D0012	Patent Counsel	(1)
Code D0271	Archive/Stock	(6)
Code D0274	Library	(2)
Code D027	M. E. Cathcart	(1)
Code D0271	D. Richter	(1)
Code D364	E. W. Jacobs	(10)
Code D805	M. S. Kvigne	(1)
Code D82	R. J. Kochanski	(1)
Code D8205	K. R. Casey	(1)
Code D824	C. R. Castro	(1)
Code D824	M. E. Stell	(1)
Code D827	L. W. Gutman	(1)
Code D827	C. W. Warner	(1)
Code D8405	B. J. Marsh	(1)
Code D8405	R. D. Peterson	(1)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (4)

NCCOSC Washington Liaison Office
Arlington, VA 22245–5200

Center for Naval Analyses
Alexandria, VA 22302–0268

Navy Acquisition, Research and Development
Information Center (NARDIC)
Arlington, VA 22244–5114

GIDEP Operations Center
Corona, CA 91718–8000